UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
WACO DIVISION

SABLE NETWORKS, INC. AND SABLE IP, LLC, ***Plaintiffs,*** v. **DELL TECHNOLOGIES INC., DELL INC., AND EMC CORPORATION,** ***Defendants.***	**Civil Action No._____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Sable Networks, Inc. and Sable IP, LLC (collectively, "Sable" or "Plaintiffs") bring this action and make the following allegations of patent infringement relating to U.S. Patent Nos.: 6,977,932 (the "'932 patent"); 7,428,209 (the "'209 patent"); 7,630,358 (the "'358 patent"); and 8,243,593 (the "'593 patent") (collectively, the "patents-in-suit"). Defendants Dell Technologies Inc., Dell Inc., and EMC Corporation (collectively, "Dell" or "Defendants") infringes the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

INTRODUCTION

1. The patents-in-suit arise from technologies developed by Dr. Lawrence G. Roberts - one of the founding fathers of the internet.[1] The patents relate to technologies for efficiently managing the flow of data packets over routers and switch devices. Dr. Roberts and engineers at Caspian Networks, Inc. and later Sable Networks, Inc. developed these technologies to address the increasing amount of data sent over computer networks.

[1] Chris Woodford, THE INTERNET: A HISTORICAL ENCYCLOPEDIA VOLUME 2 at 204 (2005) ("Widely regarded as one of the founding fathers of the Internet, Lawrence Roberts was the primary architect of ARPANET, the predecessor of the Internet.").

2. Dr. Roberts is best known for his work as the Chief Scientist of the Advanced Research Projects Agency (ARPA) where he designed and oversaw the implementation of ARPANET, the precursor to the internet. Dr. Roberts' work on ARPANET played a key role in the development of digital network transmission technologies.[2] Initially, ARPANET was used primarily to send electronic mail and Dr. Roberts developed the first program for reading and sending electronic messages.

Keenan Mayo and Peter Newcomb, *How The Web Was Won*, VANITY FAIR at 96-97 (January 7, 2009); *One of the Engineers Who Invented the Internet Wants to Build A Radical new Router,* IEEE SPECTRUM MAGAZINE (July 2009); Katie Hafner, *Billions Served Daily, and Counting*, N.Y. TIMES at G1 (December 6, 2001)("Lawrence Roberts, who was then a manager at the Advanced Research Projects Agency's Information Processing Techniques Office, solved that problem after his boss began complaining about the volume of e-mail piling up in his in box. In 1972, Dr. Roberts produced the first e-mail manager, called RD, which included a filing system, as well as a Delete function.").

3. Dr. Roberts' work on ARPANET played a key role in the development of packet switching networks. Packet switching is a digital network transmission process in which data is broken into parts which are sent independently and reassembled at a destination. Electronic messages sent over the ARPANET were broken up into packets then routed over a network to a destination. "In designing the ARPANET, Roberts expanded on the work he'd done at MIT, using

[2] Katie Hafner, *Lawrence Roberts, Who Helped Design Internet's Precursor,* N.Y. TIMES at A2 (December 31, 2018) ("Dr. Roberts was considered the decisive force behind packet switching, the technology that breaks data into discrete bundles that are then sent along various paths around a network and reassembled at their destination.").

those tiny data packets to send information from place to place."[3] Packet switching has become the primary technology for data communications over computer networks.

From Two Small Nodes, a Mighty Web Has Grown

By 1966, with these and other basic ideas in place, Lawrence Roberts, recruited by ARPA from the Massachusetts Institute of Technology, mapped out the plan. Two years after the first transmission, the number of host computers grew to 23. The @ symbol was invented in 1972, and a year later 75 percent of the Arpanet traffic was E-mail. It was starting to look like the Net.").

George Johnson, *From Two Small Nodes, a Mighty Web Has Grown*, N.Y. TIMES at F1 (October 12, 1999).

4. After leaving ARPANET, Dr. Roberts grew increasingly concerned that existing technologies for routing data packets were incapable of addressing the increasing amounts of data traversing the internet.[4] Dr. Roberts identified that as the "Net grows, the more loss and transmission of data occurs. Eventually, gridlock will set in."[5]

> ***The Internet is broken. I should know: I designed it***. In 1967, I wrote the first plan for the ancestor of today's Internet, the Advanced Research Projects Agency Network, or ARPANET, and then led the team that designed and built it. The main idea was to share the available network infrastructure by sending data as small, independent packets, which, though they might arrive at different times, would still generally make it to their destinations. The small computers that directed the data traffic-I called them Interface Message Processors, or IMPs-evolved into today's routers, and for a long time they've kept up with the Net's phenomenal growth. Until now.

[3] Code Metz, *Larry Roberts Calls Himself the Founder of The Internet. Who Are You To Argue*, WIRED MAGAZINE (September 24, 2012); John C. McDonald, FUNDAMENTALS OF DIGITAL SWITCHING at 211 (1990) ("The ARPANET was, in part, an experimental verification of the packet switching concept. Robert's objective was a new capability for resource sharing.").

[4] eWeek Editors, *Feeling A Little Congested,* EWEEK MAGAZINE (September 24, 2001) ("Lawrence Roberts, one of the primary developers of Internet precursor ARPANet and CTO of Caspian Networks, recently released research indicating that Net traffic has quadrupled during the past year alone.").

[5] Michael Cooney, *Can ATM Save The Internet,* NETWORK WORLD at 16 (May 20, 1996); Lawrence Roberts, A RADICAL NEW ROUTER, IEEE Spectrum Vol. 46 34-39 (August 2009).

Lawrence Roberts, *A Radical New Router*, IEEE SPECTRUM Vol. 46(7) at 34 (August 2009) (emphasis added).

5. In 1998, Dr. Roberts founded Caspian Networks.[6] At Caspian Networks, Dr. Roberts developed a new kind of internet router to efficiently route packets over a network. This new router was aimed at addressing concerns about network "gridlock." In a 2001 interview with Wired Magazine, Dr. Roberts discussed the router he was developing at Caspian Networks – the Apeiro. "Roberts says the Apeiro will also create new revenue streams for the carriers by solving the 'voice and video problem.' IP voice and video, unlike email and static Web pages, breaks down dramatically if there's a delay - as little as a few milliseconds - in getting packets from host to recipient."[7]

Jim Duffy, *Router Newcomers take on Cisco, Juniper*, NETWORK WORLD at 14 (April 14, 2013); Stephen Lawson, *Caspian Testing Stellar Core Offering*, NETWORK WORLD at 33 (December 17, 2001); Tim Greene, *Caspian Plans Superfast Routing For The 'Net Core*, NETWORK WORLD at 10 (January 29, 2001); Andrew P. Madden, *Company Spotlight: Caspian Networks*, MIT TECHNOLOGY REVIEW at 33 (August 2005); and Loring Wirbel, *Caspian Moves Apeiro Router To Full Availability*, EE TIMES (April 14, 2003).

[6] Caspian Networks, Inc. was founded in 1998 as Packetcom, LLC and changed its name to Caspian Networks, Inc. in 1999.

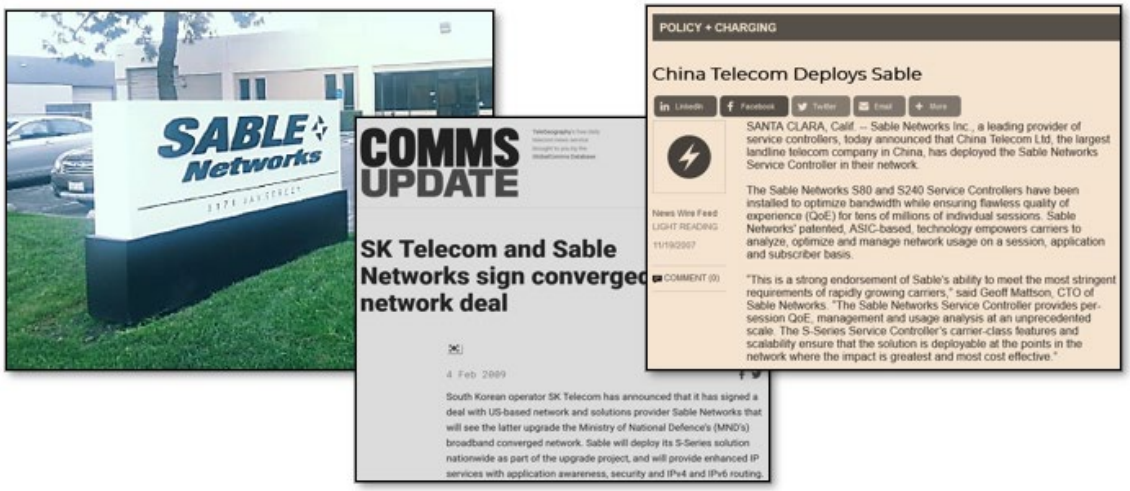
[7] John McHugh, *The n-Dimensional Superswitch*, WIRED MAGAZINE (May 1, 2001).

6. The Apeiro debuted in 2003. The Apeiro, a flow-based router, can identify the nature of a packet – be it audio, text, or video, and prioritize it accordingly. The Apeiro included numerous technological advances including quality of service (QoS) routing and flow-based routing.

7. At its height, Caspian Networks Inc. raised more than $300 million dollars and grew to more than 320 employees in the pursuit of developing and commercializing Dr. Roberts' groundbreaking networking technologies, including building flow-based routers that advanced quality of service and load balancing performance. However, despite early success with its technology and business, Caspian hit hard times when the telecommunications bubble burst.

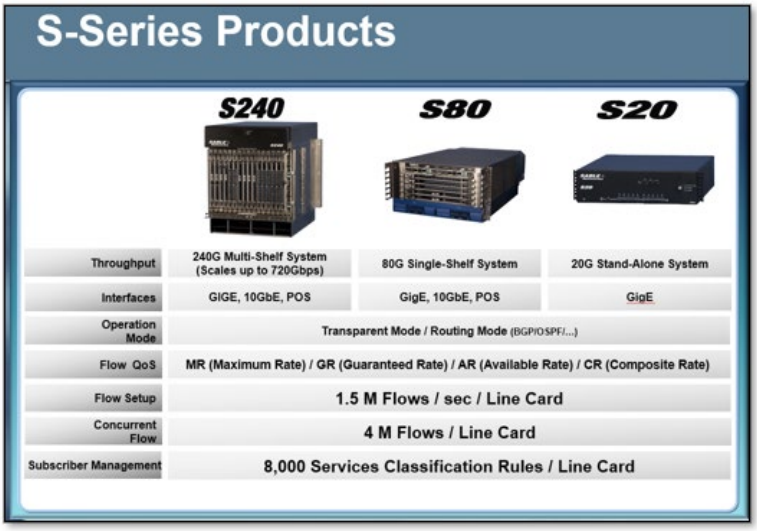
8. Sable Networks, Inc. was formed by Dr. Sang Hwa Lee to further develop and commercialize the flow-based networking technologies developed by Dr. Roberts and Caspian Networks.[8] Sable Networks, Inc. has continued its product development efforts and has gained commercial success with customers in Japan, South Korea, and China. Customers of Sable Networks, Inc. have included: SK Telecom, NTT Bizlink, Hanaro Telecom, Dacom Corporation, USEN Corporation, Korea Telecom, China Unicom, China Telecom, and China Tietong.

[8] Dr. Lee, through his company Mobile Convergence, Ltd. purchased the assets of Caspian Networks Inc. and subsequently created Sable Networks, Inc.



SK Telecom and Sable Networks Sign Convergence Network Deal, COMMS UPDATE – TELECOM NEWS SERVICE (February 4, 2009) ("South Korean operator SK Telecom has announced that it has signed a deal with US-based network and solutions provider Sable Networks."); *China Telecom Deploys Sable*, LIGHT READING NEWS FEED (November 19, 2007) ("Sable Networks Inc., a leading provider of service controllers, today announced that China Telecom Ltd, the largest landline telecom company in China, has deployed the Sable Networks Service Controller in their network.").

9. Armed with the assets of Caspian Networks Inc. as well as members of Caspian Networks' technical team, Sable Networks, Inc. continued the product development efforts stemming from Dr. Roberts' flow-based router technologies. Sable Networks, Inc. developed custom application-specific integrated circuits ("ASIC") designed for flow traffic management. Sable Network, Inc.'s ASICs include the Sable Networks SPI, which enables 20 Gigabit flow processing. In addition, Sable Networks, Inc. developed and released S-Series Service Controllers (*e.g.*, S80 and S240 Service Controller models) that contain Sable Networks' flow-based programmable ASICs, POS and Ethernet interfaces, and carrier-hardened routing and scalability from 10 to 800 Gigabits.



SABLE NETWORKS S-SERIES SERVICE CONTROLLERS (showing the S240-240G Multi-Shelf System, S80-80G Single-Shelf System, and S20-20G Stand-Alone System).

10. Sable pursues the reasonable royalties owed for Dell's use of the inventions claimed in Sable's patent portfolio, which arise from Caspian Networks and Sable Networks' groundbreaking technology.

SABLE'S PATENT PORTFOLIO

11. Sable's patent portfolio includes over 34 patent assets, including 14 granted U.S. patents. Dr. Lawrence Roberts' pioneering work on QoS traffic prioritization, flow-based switching and routing, and the work of Dr. Roberts' colleagues at Caspian Networks Inc. and Sable Networks, Inc. are claimed in the various patents owned by Sable.

12. Highlighting the importance of the patents-in-suit is the fact that the Sable's patent portfolio has been cited by over 1,000 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the computer networking field. Sable's patents have been cited by companies such as:

- Cisco Systems, Inc.[9]

[9] *See, e.g.*, U.S. Patent Nos. 7,411,965; 7,436,830; 7,539,499; 7,580,351; 7,702,765; 7,817546; 7,936,695; 8,077,721; 8,493,867; 8,868,775; and 9,013,985.

- Juniper Networks, Inc.[10]
- Broadcom Limited[11]
- EMC Corporation[12]
- F5 Networks, Inc.[13]
- Verizon Communications Inc.[14]
- Microsoft Corporation[15]
- Intel Corporation[16]
- Extreme Networks, Inc.[17]
- Huawei Technologies Co., Ltd.[18]

THE PARTIES

SABLE NETWORKS, INC.

13. Sable Networks, Inc. ("Sable Networks") is a corporation organized and existing under the laws of the State of California.

14. Sable Networks was formed to continue the research, development, and commercialization work of Caspian Networks Inc., which was founded by Dr. Lawrence Roberts to provide flow-based switching and routing technologies to improve the efficiency and quality of computer networks.

15. Sable Networks is the owner by assignment of all of the patents-in-suit.

[10] *See, e.g.*, U.S. Patent Nos. 7,463,639; 7,702,810; 7,826,375; 8,593,970; 8,717,889; 8,811,163; 8,811,183; 8,964,556; 9,032,089; 9,065,773; and 9,832,099.

[11] *See, e.g.*, U.S. Patent No. 7,187,687; 7,206,283; 7,266,117; 7,596,139; 7,649,885; 8,014,315; 8,037,399; 8,170,044; 8,194,666; 8,271,859; 8,448,162; 8,493,988; 8,514,716; and 7,657,703.

[12] *See, e.g.*, U.S. Patent Nos. 6,976,134; 7,185,062; 7,404,000; 7,421,509; 7,864,758; and 8,085,794.

[13] *See, e.g.*, U.S. Patent Nos. 7,206,282; 7,580,353; 8,418,233; 8,565,088; 9,225,479; 9,106,606; 9,130,846; 9,210,177; 9,614,772; 9,967,331; and 9,832,069.

[14] *See, e.g.*, U.S. Patent Nos. 7,349,393; 7,821,929; 8,218,569; 8,289,973; 9,282,113; and 8,913,623.

[15] *See, e.g.*, U.S. Patent Nos. 7,567,504; 7,590,736; 7,669,235; 7,778,422; 7,941,309; 7,636,917; 9,571,550; and 9,800,592.

[16] *See, e.g.*, U.S. Patent Nos. 7,177,956; 7,283,464; 9,485,178; 9,047,417; 8,718,096; 8,036,246; 8,493,852; and 8,730,984.

[17] *See, e.g.*, U.S. Patent Nos. 7,903,654; 7,978,614; 8,149839; 10,212,224; 9,112,780; and 8,395,996.

[18] *See, e.g.*, U.S. Patent Nos. 7,903,553; 7,957,421; 10,015,079; 10,505,840; and Chinese Patent Nos. CN108028828 and CN106161333.

SABLE IP, LLC

16. Sable IP, LLC ("Sable IP") is a Delaware limited liability company with its principal place of business at 225 S. 6th Street, Suite 3900, Minneapolis, Minnesota 55402. Pursuant to an exclusive license agreement with Sable Networks, Sable IP is the exclusive licensee of the patents-in-suit.

DELL DEFENDANTS

17. Dell Technologies Inc. is a Delaware corporation with its principal place of business at One Dell Way, Round Rock, Texas 78682. Dell Technologies Inc. may be served through its registered agent Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808.

18. Dell Inc. is a Delaware corporation with a principal place of business at One Dell Way, Round Rock, Texas 78682. Dell Inc. may be served through its registered agent Corporation Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701. Dell Inc. is registered to do business in the State of Texas and has been since at least October 27, 1987. In addition to its corporate headquarters in Round Rock, Texas, Defendant Dell Inc. maintains several other offices in this District, including offices at 12500 Tech Ridge Blvd., Bldg. PS4, Austin, Texas 78753; 1404 Park Center Dr., Austin, Texas 78754; 4309 Emma Browning Ave., Austin, Texas 78719; 600 Congress Ave., Austin, Texas 78701; 701 E. Parmer Lane, Bldg. PS2, Austin, Texas 78753; 9715 Burnet Road, Metric – 7, Suite 300, Austin, Texas 78758; 5822 Cromo Drive, El Paso, Texas 79912; 200 Dell Way, Round Rock, Texas 78758; 2300 Greenlawn Blvd., Round Rock, Texas 78682; 401 Dell Way, Round Rock, Texas 78682; 501 Dell Way, Round Rock, Texas 78682; and 9830 Colonnade Blvd., Suite 380, San Antonio, Texas 78230.

19. EMC Corporation is a Massachusetts corporation with a principal place of business at One Dell Way, Round Rock, Texas 78682. EMC Corporation may be served through its

registered agent Corporation Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701. EMC Corporation is registered to do business in the State of Texas and has been since at least July 17, 1987. In addition to its corporate headquarters in Round Rock, Texas, on information and belief, EMC Corporation operates out of multiple offices in this District.

JURISDICTION AND VENUE

20. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

21. This Court has personal jurisdiction over Dell in this action because Dell has committed acts within the Western District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Dell would not offend traditional notions of fair play and substantial justice. Dell, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Dell Inc. and EMC Corporation are registered to do business in the State of Texas. Each of the Defendants is headquartered in this District, and Dell Inc. and EMC Corporation each maintain multiple office locations in this District. Further, Dell actively directs its activities to customers located in the State of Texas.

22. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Dell is headquartered in this District, has transacted business in the Western District of Texas, and has committed acts of direct and indirect infringement in the Western District of Texas.

23. Defendants also each have a regular and established place of business in this District and have committed acts of infringement in this District. Dell has also committed acts of

infringement in this District by commercializing, marketing, selling, distributing, testing, and servicing certain accused products.

24. This Court has personal jurisdiction over Dell. Dell has conducted and does conduct business within the State of Texas. Dell, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ships, distributes, makes, uses, offers for sale, sells, imports, and/or advertises (including by providing an interactive web page) its products and/or services in the United States and the Western District of Texas and/or contributes to and actively induces its customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the provision of an interactive web page) infringing products and/or services in the United States and the Western District of Texas. Dell, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), has purposefully and voluntarily placed one or more of its infringing products and/or services, as described below, into the stream of commerce with the expectation that those products will be purchased and used by customers and/or consumers in the Western District of Texas. These infringing products and/or services have been and continue to be made, used, sold, offered for sale, purchased, and/or imported by customers and/or consumers in the Western District of Texas. Dell has committed acts of patent infringement within the Western District of Texas. Dell interacts with customers in Texas, including through visits to customer sites in Texas. Through these interactions and visits, Dell directly infringes the patents-in-suit. Dell also interacts with customers who sell the Accused Products into Texas, knowing that these customers will sell the Accused Products into Texas, either directly or through intermediaries.

25. Dell has minimum contacts with this District such that the maintenance of this action within this District would not offend traditional notions of fair play and substantial justice. Thus, the Court therefore has both general and specific personal jurisdiction over Dell.

THE ASSERTED PATENTS

U.S. PATENT NO. 6,977,932

26. U.S. Patent No. 6,977,932 (the "'932 patent") entitled, *System and Method for Network Tunneling Utilizing Micro-Flow State Information*, was filed on January 16, 2002. The '932 patent is subject to a 35 U.S.C. § 154(b) term extension of 815 days. Sable Networks, Inc. is the owner by assignment of the '932 patent. Sable IP is the exclusive licensee of the '932 patent. A true and correct copy of the '932 patent is attached hereto as Exhibit A.

27. The '932 patent discloses novel methods and apparatuses for utilizing a router capable of network tunneling utilizing flow state information.

28. The inventions disclosed in the '932 patent enable the use of micro-flow state information to improve network tunneling techniques.

29. The inventions disclosed in the '932 patent maintain flow state information for various quality of service characteristics by utilizing aggregate flow blocks.

30. The aggregate flow blocks disclosed in the '932 patent maintain micro-flow block information.

31. The technologies claimed in the '932 patent speed the flow of network traffic over computer networks by avoiding time consuming and processor intensive tasks by combining flow state information with other information such as label switched paths utilization information. This permits the micro-flows associated with an aggregate flow block to all be processed in a similar manner.

32. The technologies disclosed in the '932 patent result in more efficient computer networks by avoiding the processor intensive tasks of searching millions of flow blocks to identify flow blocks having certain micro-flow characteristics in order to process large numbers of micro-flows.

33. The '932 patent discloses a router capable of network tunneling utilizing flow state information containing an aggregate flow block having tunnel specific information for a particular network tunnel.

34. The '932 patent discloses a router capable of network tunneling utilizing flow state information containing a flow block having flow state information for a micro-flow, the flow block further including an identifier that associates the flow block with the aggregate flow block.

35. The '932 patent discloses a router capable of network tunneling utilizing flow state information wherein the aggregate flow block stores statistics for the particular network tunnel.

36. The '932 patent has been cited by 86 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '932 patent as relevant prior art:

- Cisco Systems, Inc.
- Juniper Networks, Inc.
- Avaya, Inc.
- Fujitsu, Ltd.
- Intel Corporation
- Nokia Corporation
- Qualcomm, Inc.
- Sprint Communications Co.
- Telefonaktiebolaget LM Ericsson
- Verizon Communications, Inc.

U.S. PATENT NO. 7,428,209

37. U.S. Patent No. 7,428,209 (the "'209 patent") entitled, *Network Failure Recovery Mechanism*, was filed on June 12, 2001. The '209 patent is subject to a 35 U.S.C. § 154(b) term

extension of 655 days. Sable Networks, Inc. is the owner by assignment of the '209 patent. Sable IP is the exclusive licensee of the '209 patent. A true and correct copy of the '209 patent is attached hereto as Exhibit B.

38. The '209 patent discloses novel methods and systems for implementing within a network router a method for recovering from a failure.

39. The inventions disclosed in the '209 patent enable large-scale computer networks to quickly recover from a component failure.

40. The '209 patent discloses a method implemented on a network router that recovers from a failure.

41. The '209 patent discloses a method implemented on a network router for sending, via a first route, a first set of information from an ingress module to a first egress module for forwarding by the first egress module to a destination external to the router, where a first set of information traverses a path which encompasses at least a portion of the first route.

42. The '209 patent discloses a method implemented on a network router for detecting an external failure beyond the first egress module.

43. The '209 patent discloses a method implemented on a network router for directing a message to the ingress module informing the ingress module of the external failure in response to an external failure.

44. The '209 patent discloses a method implemented on a network router for selecting an alternate egress module capable of forwarding information to a destination in response to an error message.

45. The '209 patent discloses a method implemented on a network router for sending, via a second route, a future set of information from the ingress module to the alternate egress

module for forwarding to the destination, where the first set of information and the future set of information are both part of a flow.

46. The '209 patent discloses a method implemented on a network router for causing other sets of information associated with the flow to be sent from the ingress module to the alternate egress module in response to the message.

47. The '209 patent discloses a method implemented on a network router for directing to the ingress module that comprises: (1) identifying the ingress module; (2) accessing a routing table which comprises one or more routes to the ingress module; (3) obtaining a return route from the routing table, wherein the return route directs the message to the ingress module along a different path than that traversed by said first set of information; and (4) sending a message to the ingress module via the return route.

48. The '209 patent discloses a method implemented on a network router where the first egress module and the alternate egress module are predetermined, where identifiers associated with the first egress module and the alternate egress module are stored within a flow block associated with the flow. Further, the '209 patent teaches storing an indication in the flow block that all sets of information associated with the flow are to be sent to the alternate egress module.

49. The '209 patent family has been cited by 52 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '209 patent family as relevant prior art:

- Cisco Systems, Inc.
- AT&T, Inc.
- Canon, Inc.
- British Telecommunications Public Limited Co.
- ***EMC Corporation***
- Hewlett Packard Enterprise Company
- Infinera Corporation
- International Business Machines Corporation

- ShoreTel, Inc.
- Nokia Corporation
- Monarch Networking Solutions LLC

U.S. PATENT NO. 7,630,358

50. U.S. Patent No. 7,630,358 ("the '358 patent") entitled, *Mechanism for Implementing Multiple Logical Routers Within A Single Physical Router*, was filed on July 9, 2002, and claims priority to July 9, 2001. The '358 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,136 days. Sable Networks, Inc. is the owner by assignment of the '358 patent. Sable IP is the exclusive licensee of the '358 patent. A true and correct copy of the '358 patent is attached hereto as Exhibit C.

51. The '358 patent claims specific methods and systems for implementing multiple logical routers within a single physical router.

52. The '358 patent discloses systems and methods that combine the benefits of multi-routers and virtual routers. The logical routers are included within the same physical router; however, internal links permit improved efficiency over virtual routers because the technologies claimed in the '358 patent can take advantage of the fact that the logical routers are not standalone routers bur are embodied in the same physical router.

53. The '358 patent discloses technology for implementing multiple logical routers within a single physical router.

54. The '358 patent discloses a router with a first set of one or more components capable of being figured to implement a first logical router within the router.

55. The '358 patent discloses a router with a second set of one or more components capable of being configured to implement a second logical router within the router.

56. The '358 patent discloses a router with a forwarding routing table that comprises an identifier that indicates an internal link is internal rather than an external link.

57. The '358 patent discloses a router wherein the first and second sets of components comprise functionality for establishing the internal link between the first logical router and the second logical router and advertising the internal link to other routers external to the router such that the first and second logical routers appear to the other routers as interconnected standalone routers, wherein the internal link is a logical, non-physical entity.

58. The '358 patent has been cited by 42 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have all cited the '358 patent as relevant prior art:

- Cisco Systems, Inc.
- Dell Technologies, Inc.
- Juniper Networks, Inc.
- Nicira, Inc.
- International Business Machines Corporation
- NantWorks, LLC
- Telefonaktiebolaget LM Ericsson
- Verizon Communications, Inc.

U.S. PATENT NO. 8,243,593

59. U.S. Patent No. 8,243,593 entitled, *Mechanism for Identifying and Penalizing Misbehaving Flows in a Network*, was filed on December 22, 2004. The '593 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,098 days. Sable Networks, Inc. is the owner by assignment of the '593 patent. Sable IP is the exclusive licensee of the '593 patent. A true and correct copy of the '593 patent is attached hereto as Exhibit D.

60. The '593 patent discloses novel methods and systems for processing a flow of a series of information packets.

61. The inventions disclosed in the '593 patent teach technologies that permit the identification and control of less desirable network traffic.

62. Because the characteristics of data packets in undesirable network traffic can be disguised, the '593 patent improves the operation of computer networks by disclosing technologies that monitor the characteristics of flows of data packets rather than ancillary factors such as port numbers or signatures.

63. The '593 patent discloses tracking the behavioral statistics of a flow of data packets that can be used to determine whether the flow is undesirable.

64. The '593 patent further discloses taking actions to penalize the flow of undesirable network traffic.

65. The '593 patent discloses a method for processing a flow of a series of information packets that maintains a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

66. The '593 patent discloses a method for processing a flow of a series of information packets that determines, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

67. The '593 patent discloses that the determination as to whether the flow is exhibiting undesirable behavior is made regardless of the presence or absence of congestion.

68. The '593 patent discloses a method for processing a flow of data packets that enforces a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

69. The '593 patent has been cited by 17 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '593 patent as relevant prior art.

- Cisco Systems, Inc.
- AT&T, Inc.
- International Business Machines Corporation
- Telecom Italia S.p.A.
- McAfee, LLC

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 6,977,932

70. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

71. Dell designs, makes, sells, offers to sell, imports, and/or uses the following products: Dell EMC PowerSwitch N1500 Series devices (1524, 1524P, 1548, 1548P); Dell EMC PowerSwitch N2000 Series devices (2024, 2024P, 2048, 2048P); Dell EMC PowerSwitch N3000 Series devices (3024, 3024P, 3048, 3048P); and Dell EMC PowerSwitch N4000 Series devices (4032, 4032F, 4064, 4064F) (collectively, the "Dell '932 Products(s)").

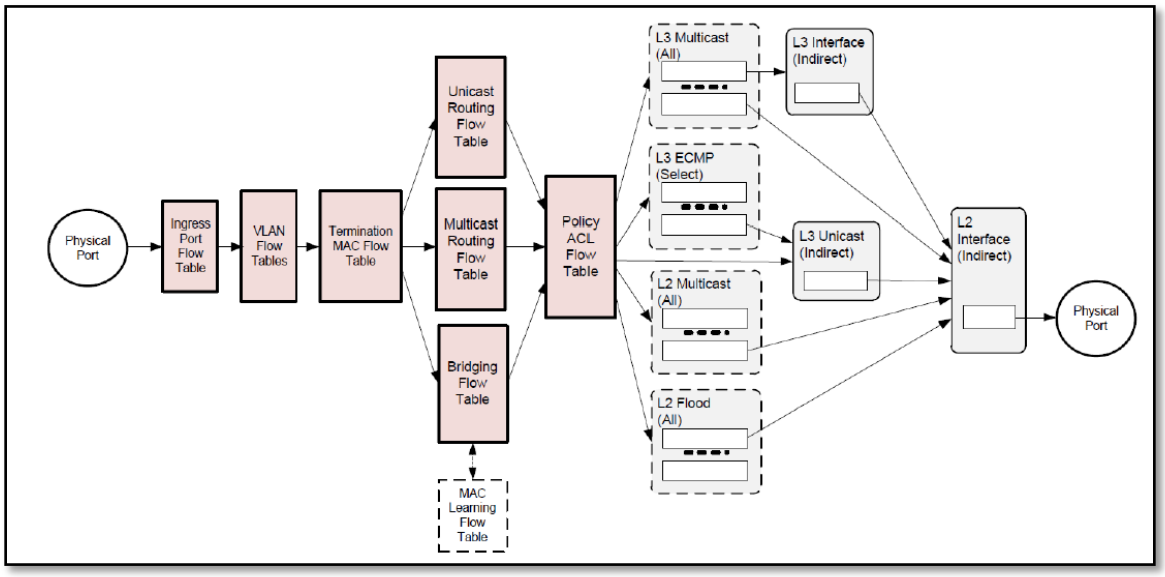
72. One or more Dell subsidiaries and/or affiliates use the Dell '932 Products in regular business operations.

73. Dell has directly infringed and continues to directly infringe the '932 patent by, among other things, making, using, offering for sale, and/or selling technology that utilize flow state information to perform a method of network tunneling.

74. One or more of the Dell '932 Products utilize flow state information to perform a network tunneling method.

75. One or more of the Dell '932 Products create a flow block having flow state information for a received first data packet of a micro-flow. The following figure shows that data

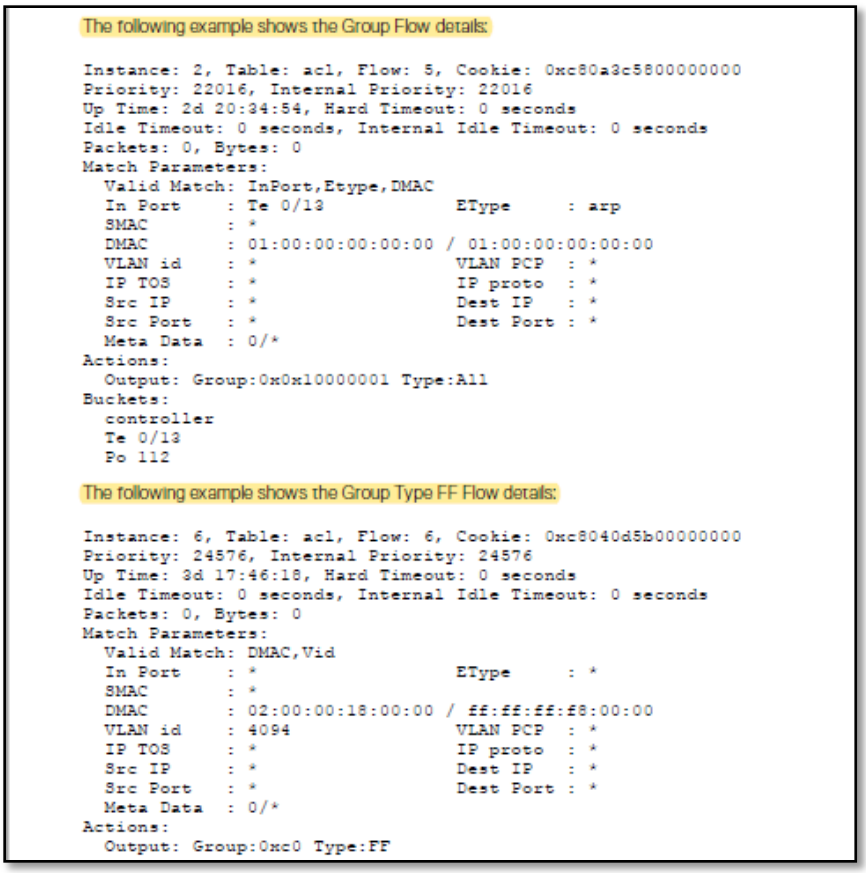
packets are received at an ingress port and processed using the ingress port flow table which is associated with routing tables such as the "Unicast Routing Flow Table" and "Multicast Routing Flow Table"



Dell Networking Operating System for OpenFlow on N-Series (DNOS-OF), DELL USER GUIDE V1.1B at 15 (June 2016).

76. One or more of the Dell '932 Products store a tunnel identifier for the micro-flow in the flow block, the tunnel identifier identifying a selected network tunnel to be used to transmit the data packet.

77. One or more of the Dell '932 Products index an aggregate flow block using the tunnel identifier. The following excerpt from Dell documentation describes the use of Group Flows and Group Type FF Flows.



The following example shows the Group Flow details:

```
Instance: 2, Table: acl, Flow: 5, Cookie: 0xc80a3c5800000000
Priority: 22016, Internal Priority: 22016
Up Time: 2d 20:34:54, Hard Timeout: 0 seconds
Idle Timeout: 0 seconds, Internal Idle Timeout: 0 seconds
Packets: 0, Bytes: 0
Match Parameters:
  Valid Match: InPort,Etype,DMAC
  In Port     : Te 0/13             EType      : arp
  SMAC        : *
  DMAC        : 01:00:00:00:00:00 / 01:00:00:00:00:00
  VLAN id     : *                   VLAN PCP   : *
  IP TOS      : *                   IP proto   : *
  Src IP      : *                   Dest IP    : *
  Src Port    : *                   Dest Port  : *
  Meta Data   : 0/*
Actions:
  Output: Group:0x0x10000001 Type:All
Buckets:
  controller
  Te 0/13
  Po 112
```

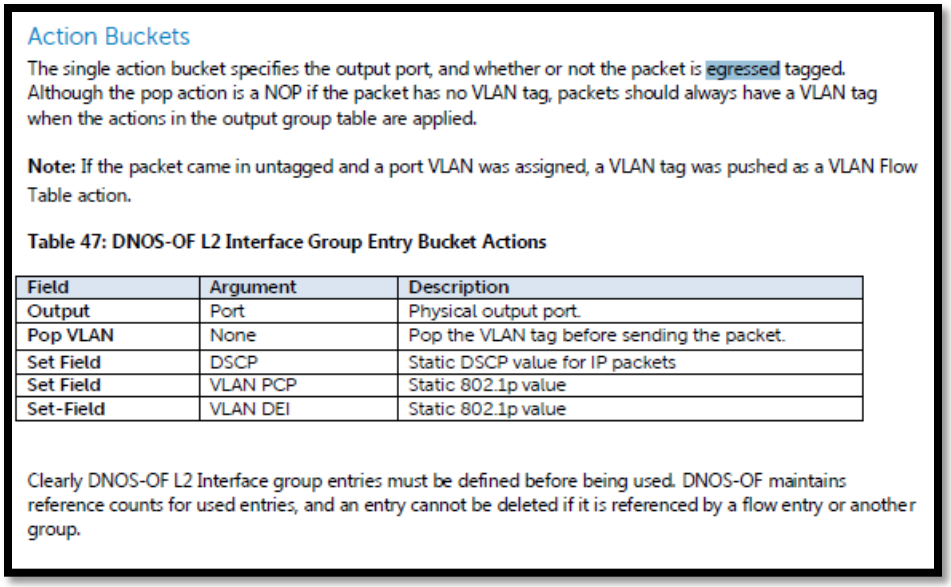
The following example shows the Group Type FF Flow details:

```
Instance: 6, Table: acl, Flow: 6, Cookie: 0xc8040d5b00000000
Priority: 24576, Internal Priority: 24576
Up Time: 3d 17:46:18, Hard Timeout: 0 seconds
Idle Timeout: 0 seconds, Internal Idle Timeout: 0 seconds
Packets: 0, Bytes: 0
Match Parameters:
  Valid Match: DMAC,Vid
  In Port     : *                   EType      : *
  SMAC        : *
  DMAC        : 02:00:00:18:00:00 / ff:ff:ff:f8:00:00
  VLAN id     : 4094                VLAN PCP   : *
  IP TOS      : *                   IP proto   : *
  Src IP      : *                   Dest IP    : *
  Src Port    : *                   Dest Port  : *
  Meta Data   : 0/*
Actions:
  Output: Group:0xc0 Type:FF
```

Dell OpenFlow Deployment and User Guide 4.0 – Dell Software Defined Networking (SDN), DELL DOCUMENTATION at 22 (January 2017) (emphasis added).

78. One or more of the Dell '932 Products utilize an aggregate flow block with tunnel specific information for the selected network tunnel and that stores statistics for the selected network tunnel.

79. One or more of the Dell '932 Products transmit data packets using the selected network tunnel based on the tunnel specific information. The Dell '932 Products enable the use of action buckets wherein a packet can be transmitted on. For example, if a packet comes in and as part of the flow processing a VLAN is assigned a VLAN tag is bushed as a VLAN Flow Table action.



Action Buckets

The single action bucket specifies the output port, and whether or not the packet is egressed tagged. Although the pop action is a NOP if the packet has no VLAN tag, packets should always have a VLAN tag when the actions in the output group table are applied.

Note: If the packet came in untagged and a port VLAN was assigned, a VLAN tag was pushed as a VLAN Flow Table action.

Table 47: DNOS-OF L2 Interface Group Entry Bucket Actions

Field	Argument	Description
Output	Port	Physical output port.
Pop VLAN	None	Pop the VLAN tag before sending the packet.
Set Field	DSCP	Static DSCP value for IP packets
Set Field	VLAN PCP	Static 802.1p value
Set-Field	VLAN DEI	Static 802.1p value

Clearly DNOS-OF L2 Interface group entries must be defined before being used. DNOS-OF maintains reference counts for used entries, and an entry cannot be deleted if it is referenced by a flow entry or another group.

Dell Networking Operating System for OpenFlow on N-Series (DNOS-OF), DELL USER GUIDE V1.1B at 34 (June 2016).

80. The Dell '932 Products are available to businesses and individuals throughout the United States.

81. The Dell '932 Products are provided to businesses and individuals located in the Western District of Texas.

82. By making, using, testing, offering for sale, and/or selling products utilizing flow state information to perform a method of network tunneling, including but not limited to the Dell '932 Products, Dell has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '932 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

83. Dell also indirectly infringes the '932 patent by actively inducing infringement under 35 USC § 271(b).

84. Dell has had knowledge of the '932 patent since at least service of this Complaint or shortly thereafter, and Dell knew of the '932 patent and knew of its infringement, including by way of this lawsuit.

85. Dell intended to induce patent infringement by third-party customers and users of the Dell '932 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Dell specifically intended and was aware that the normal and customary use of the accused products would infringe the '932 patent. Dell performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '932 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell provides the Dell '932 Products that have the capability of operating in a manner that infringe one or more of the claims of the '932 patent, including at least claim 1, and Dell further provides documentation and training materials that cause customers and end users of the Dell '932 Products to utilize the products in a manner that directly infringe one or more claims of the '932 patent.[19] By providing instruction and training to customers and end-users on how to use the Dell '932 Products in a manner that directly infringes one or more claims of the '932 patent, including at least claim 1, Dell specifically intended to induce infringement of the '932 patent. Dell engaged in such inducement to promote the sales of the Dell '932 Products, e.g., through Dell user manuals, product support, marketing materials, and

[19] *See, e.g.*, *Dell EMC Networking N4000 Series Switches,* DELL DATASHEET (May 2017); *Dell Networking N-Series N1500, N2000, N3000, and N4000 Switches,* DELL USER'S CONFIGURATION GUIDE VERSION 6.3.0.0 (January 2016); *Dell Networking N4000 Series and Dell PowerConnect 8100 Series – Switch Configuration Guide for EqualLogic SANs*, DELL DOCUMENTATION (March 2014); *Dell Networking N2000 Series Switches,* DELL DATASHEET (November 2013); *Dell EMC Networking N-Series: N1100-ON, N1500, N2000, N2100-ON, N3000, N3100-ON, and N4000 Switches CLI Reference Guide*, DELL DOCUMENTATION (November 2018); *OpenFlow Single-table Implementation for Dell Networking N-Series SDN*, DELL DEPLOYMENT AND CONFIGURATION GUIDE (October 2016); *Dell Networking Operating System for OpenFlow on N-Series (DNOS-OF)*, DELL USER GUIDE V1.1B (June 2016); *Dell Software-Defined Networking (SDN Deployment Guide Version 1.0,* DELL DOCUMENTATION (2013); *Dell EMC SmartFabric OS10 User Guide*, *Release 10.5.0,* DELL DOCUMENTATION (September 2019); *Deploying Dell Networking and Configuring SDN*, DELL EMC SUPPORT YOUTUBE CHANNEL (September 2013), *available at*: https://www.youtube.com/watch?v=P5gtKAocOIo; and *5.0 Firmware Update For Dell PowerConnect Switches*, DELL EMC SUPPORT YOUTUBE CHANNEL (August 2012), *available at*: https://www.youtube.com/watch?v=ySD5QhbbIhw.

training materials to actively induce the users of the accused products to infringe the '932 patent. Accordingly, Dell has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '932 patent, knowing that such use constitutes infringement of the '932 patent.

86. The '932 patent is well-known within the industry as demonstrated by multiple citations to the '932 patent in published patents and patent applications assigned to technology companies and academic institutions. Dell is utilizing the technology claimed in the '932 patent without paying a reasonable royalty. Dell is infringing the '932 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

87. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '932 patent.

88. As a result of Dell's infringement of the '932 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Dell's infringement, but in no event less than a reasonable royalty for the use made of the invention by Dell together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 7,428,209

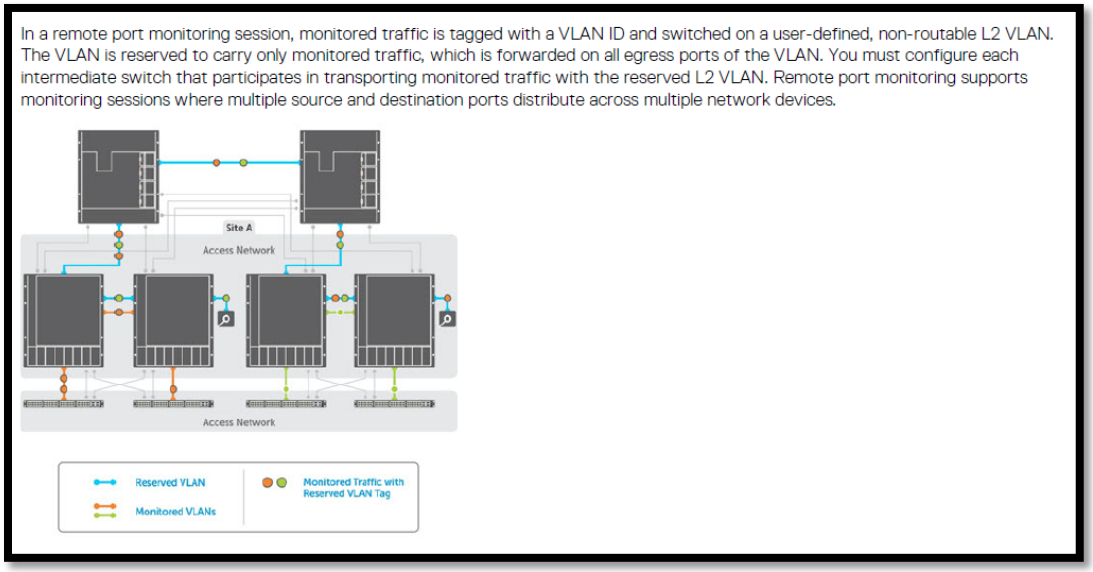
89. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

90. Dell designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for implementing within a network router a method for recovering from a failure.

91. Dell designs, makes, sells, offers to sell, imports, and/or uses Dell EMC PowerEdge MX infrastructure products with the Dell EMC SmartFabric OS10 or later network operating system (collectively, the "Dell '209 Products").

92. One or more Dell subsidiaries and/or affiliates use the Dell '209 Products in regular business operations.

93. One or more of the Dell '209 Products include technology for implementing within a network router a method for recovering from a failure. The below excerpt from Dell documentation shows a configuration of the Dell '209 products wherein the egress modules are connected to external locations.

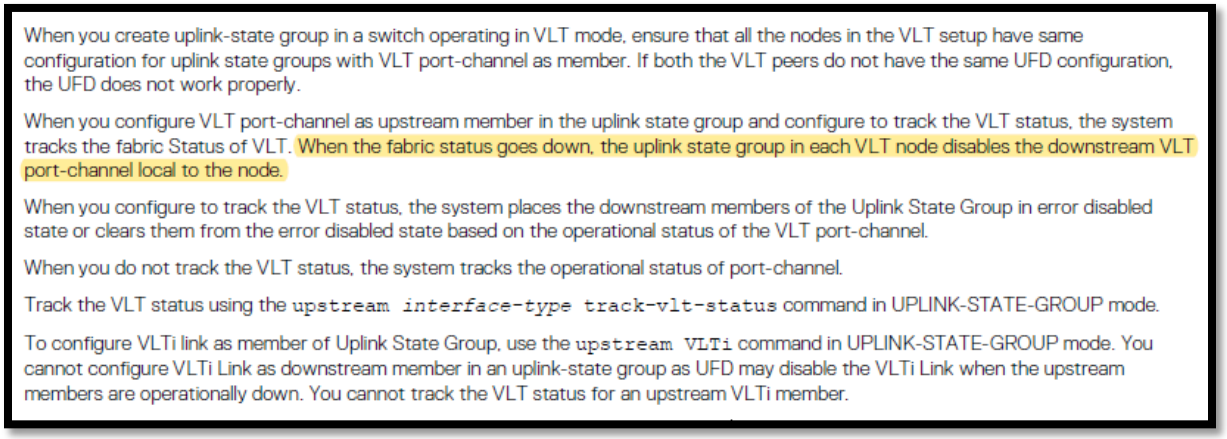


Dell EMC SmartFabric OS10 User Guide, Release 10.5.0, DELL DOCUMENTATION at 471 (2020).

94. One or more of the Dell '209 Products include technology for sending, via a first route, a first set of information from an ingress module to a first egress module for forwarding by said first egress module to a destination external to said router, wherein said first set of information traverses a path which encompasses at least a portion of said first route.

95. One or more of the Dell '209 Products include technology for sending, via a first route, a first set of information from an ingress module to a first egress module for forwarding by said first egress module to a destination external to said router, wherein said first set of information traverses a path which encompasses at least a portion of said first route.

96. The Dell '209 Products enable the use of "Uplink Failure Detection" with "Virtual Link Trunking." Dell documentation states when the status of an uplink connection goes down "the uplink state group in each VLT node disables the downstream VLT port-channel local to the node." Further, when the event "VLTi Link is operationally down with heartbeat up" the VLT module sends the VLT port channel disable request to the Interface Manager ("IFM") for both the uplink and downlink.



When you create uplink-state group in a switch operating in VLT mode, ensure that all the nodes in the VLT setup have same configuration for uplink state groups with VLT port-channel as member. If both the VLT peers do not have the same UFD configuration, the UFD does not work properly.

When you configure VLT port-channel as upstream member in the uplink state group and configure to track the VLT status, the system tracks the fabric Status of VLT. When the fabric status goes down, the uplink state group in each VLT node disables the downstream VLT port-channel local to the node.

When you configure to track the VLT status, the system places the downstream members of the Uplink State Group in error disabled state or clears them from the error disabled state based on the operational status of the VLT port-channel.

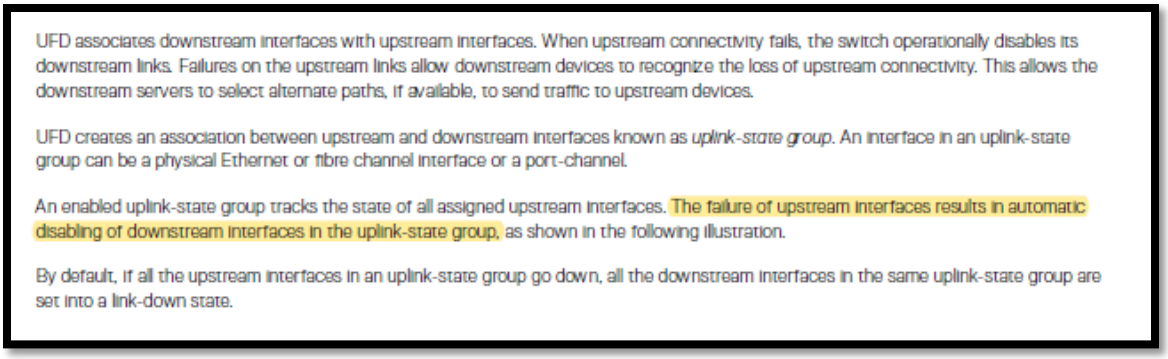
When you do not track the VLT status, the system tracks the operational status of port-channel.

Track the VLT status using the `upstream interface-type track-vlt-status` command in UPLINK-STATE-GROUP mode.

To configure VLTi link as member of Uplink State Group, use the `upstream VLTi` command in UPLINK-STATE-GROUP mode. You cannot configure VLTi Link as downstream member in an uplink-state group as UFD may disable the VLTi Link when the upstream members are operationally down. You cannot track the VLT status for an upstream VLTi member.

Dell EMC SmartFabric OS10 User Guide, Release 10.5.0, DELL DOCUMENTATION at 1230 (2020) (emphasis added).

97. One or more of the Dell '209 Products include technology for detecting a failure of said first egress module.



UFD associates downstream interfaces with upstream interfaces. When upstream connectivity fails, the switch operationally disables its downstream links. Failures on the upstream links allow downstream devices to recognize the loss of upstream connectivity. This allows the downstream servers to select alternate paths, if available, to send traffic to upstream devices.

UFD creates an association between upstream and downstream interfaces known as *uplink-state group*. An interface in an uplink-state group can be a physical Ethernet or fibre channel interface or a port-channel.

An enabled uplink-state group tracks the state of all assigned upstream interfaces. The failure of upstream interfaces results in automatic disabling of downstream interfaces in the uplink-state group, as shown in the following illustration.

By default, if all the upstream interfaces in an uplink-state group go down, all the downstream interfaces in the same uplink-state group are set into a link-down state.

Dell EMC OS10 Enterprise Edition User Guide, Release 10.4.0E(R3), DELL DOCUMENTATION at 476 (May 2018) (emphasis added).

98. One or more of the Dell '209 Products include technology for directing a message to said ingress module informing said ingress module of said first egress module failure in response to said failure of said first egress module.

99. One or more of the Dell '209 Products include technology for selecting an alternate egress module capable of forwarding information to said destination in response to said message.

100. One or more of the Dell '209 Products include technology for sending, via a second route, a future set of information from said ingress module to said alternate egress module for forwarding to said destination, wherein said first set of information and said future set of information are both part of a flow.

101. One or more of the Dell '209 Products include technology for preventing other sets of information associated with said flow from being sent from said ingress module to said first egress module in response to said message.

102. One or more of the Dell '209 Products include technology wherein directing said message to said ingress module comprises: (1) identifying said ingress module, (2) accessing a routing table which comprises one or more routes to said ingress module, (3) obtaining a return route from said routing table, wherein said return route directs said message to said ingress module

along a different path than that traversed by said first set of information, and (4) sending said message to said ingress module via said return route.

103. One or more of the Dell '209 Products include technology wherein the first egress module and said alternate egress module are predetermined.

104. One or more of the Dell '209 Products include technology wherein identifiers associated with said first egress module and said alternate egress module are stored within a flow block associated with said flow.

105. One or more of the Dell '209 Products include technology wherein the above-described preventing comprises storing an identification in said flow block that all sets of information associated with said flow are not to be sent to said first egress module.

106. Dell has directly infringed and continues to directly infringe the '209 patent by, among other things, making, using, offering for sale, and/or selling technology for implementing within a network router a method for recovering from a failure, including but not limited to the Dell '209 Products.

107. The Dell '209 Products are available to businesses and individuals throughout the United States.

108. The Dell '209 Products are provided to businesses and individuals located in the Western District of Texas.

109. By making, using, testing, offering for sale, and/or selling products and services for implementing within a network router a method for recovering from a failure, including but not limited to the Dell '209 Products, Dell has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '209 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

110. Dell also indirectly infringes the '209 patent by actively inducing infringement under 35 USC § 271(b).

111. Dell has had knowledge of the '209 patent since at least service of this Complaint or shortly thereafter, and Dell knew of the '209 patent and knew of its infringement, including by way of this lawsuit.

112. Alternatively, Dell has had knowledge of the '209 patent since at least December 27, 2011, based on its citation of the '209 patent as relevant prior art during the prosecution of the application leading to U.S. Patent No. 8,085,794, which is assigned to EMC Corporation and issued on December 27, 2011.

113. Dell intended to induce patent infringement by third-party customers and users of the Dell '209 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Dell specifically intended and was aware that the normal and customary use of the accused products would infringe the '209 patent. Dell performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '209 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell provides the Dell '209 Products that have the capability of operating in a manner that infringe one or more of the claims of the '209 patent, including at least claim 1, and Dell further provides documentation and training materials that cause customers and end users of the Dell '209 Products to utilize the products in a manner that directly infringe one or more claims of the '209 patent.[20] By providing instruction and training to

[20] *See, e.g.*, *PowerEdge MX-Series Fabric Management*, DELL DOCUMENTATION (2018); *Dell EMC Networking MXG610s Fibre Channel Switch, Fibre Channel IO Module MX7000 Chassis Deployments*, DELL DOCUMENTATION (2018); *Dell EMC PowerEdge MX SmartFabric Deployment Guide,* DELL DOCUMENTATION (November 2018); *Dell EMC SmartFabric OS10 User Guide, Release 10.5.0,* DELL DOCUMENTATION (2020); *Dell EMC OpenManage Enterprise-Modular Edition Version 1.10.20 for PowerEdge MX7000 Chassis User's Guide*,

customers and end-users on how to use the Dell '209 Products in a manner that directly infringes one or more claims of the '209 patent, including at least claim 1, Dell specifically intended to induce infringement of the '209 patent. Dell engaged in such inducement to promote the sales of the Dell '209 Products, e.g., through Dell user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '209 patent. Accordingly, Dell has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '209 patent, knowing that such use constitutes infringement of the '209 patent.

114. The '209 patent is well-known within the industry as demonstrated by multiple citations to the '209 patent in published patents and patent applications assigned to technology companies and academic institutions. Dell is utilizing the technology claimed in the '209 patent without paying a reasonable royalty. Dell is infringing the '209 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

115. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '209 patent.

116. As a result of Dell's infringement of the '209 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Dell's infringement, but in no event less than a reasonable royalty for the use made of the invention by Dell together with interest and costs as fixed by the Court.

DELL DOCUMENTATION (2020); *Dell EMC PowerEdge MX Networking Architecture Guide,* DELL DOCUMENTATION (October 2019); *Dell PowerEdge FN I/O Aggregator Configuration Guide 9.6(0.0),* DELL DOCUMENTATION (September 2019); *Dell EMC OS10 Enterprise Edition User Guide, Release 10.4.0E(R3)*, DELL DOCUMENTATION (May 2018); and *Dell EMC PowerEdge MX SmartFabric Deployment*, DELL EMC YOUTUBE.COM CHANNEL (September 20, 2018); available at: https://www.youtube.com/watch?v=qjjyV5hdTMo.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,630,358

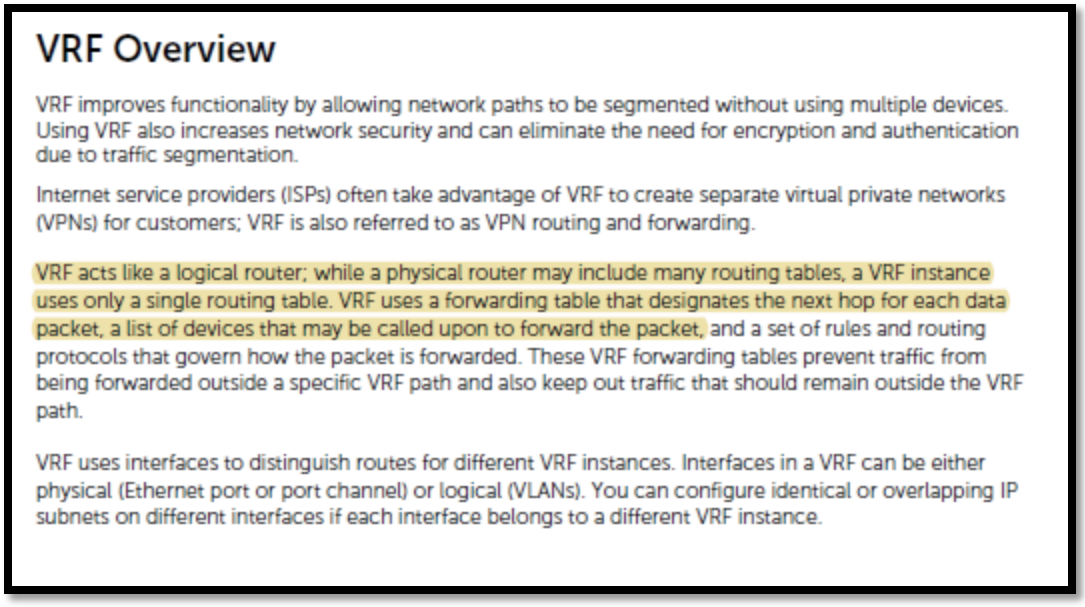
117. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

118. Dell designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for implementing multiple logical routers within a single physical router.

119. Dell designs, makes, sells, offers to sell, imports, and/or uses Dell EMC PowerSwitch devices with the Dell EMC Networking OS10 or later network operating system, which include: Dell EMC PowerSwitch S-Series devices (S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148FE-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S5148F-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, S6010-ON) and Dell EMC PowerSwitch Z-Series devices (Z9100-ON, Z9264F-ON) (collectively, the "Dell '358 Products(s)").

120. One or more Dell subsidiaries and/or affiliates use the Dell '358 Products in regular business operations.

121. One or more of the Dell '358 Products include technology for implementing multiple logical routers within a single physical router.



VRF Overview

VRF improves functionality by allowing network paths to be segmented without using multiple devices. Using VRF also increases network security and can eliminate the need for encryption and authentication due to traffic segmentation.

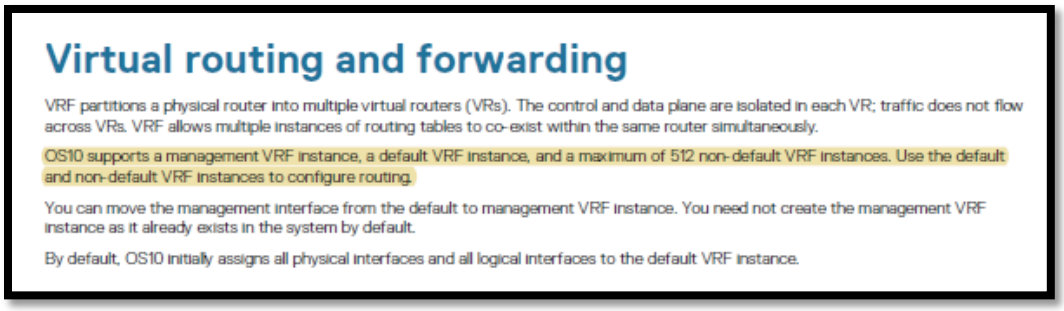
Internet service providers (ISPs) often take advantage of VRF to create separate virtual private networks (VPNs) for customers; VRF is also referred to as VPN routing and forwarding.

VRF acts like a logical router; while a physical router may include many routing tables, a VRF instance uses only a single routing table. VRF uses a forwarding table that designates the next hop for each data packet, a list of devices that may be called upon to forward the packet, and a set of rules and routing protocols that govern how the packet is forwarded. These VRF forwarding tables prevent traffic from being forwarded outside a specific VRF path and also keep out traffic that should remain outside the VRF path.

VRF uses interfaces to distinguish routes for different VRF instances. Interfaces in a VRF can be either physical (Ethernet port or port channel) or logical (VLANs). You can configure identical or overlapping IP subnets on different interfaces if each interface belongs to a different VRF instance.

Dell Networking Configuration Guide for the C9000 Series Version 9.9(0.0), DELL DOCUMENTATION at 1051 (October 2015) (emphasis added).

122. One or more of the Dell '358 Products include a router with a first set of one or more components capable of being figured to implement a first logical router within the router.



Virtual routing and forwarding

VRF partitions a physical router into multiple virtual routers (VRs). The control and data plane are isolated in each VR; traffic does not flow across VRs. VRF allows multiple instances of routing tables to co-exist within the same router simultaneously.

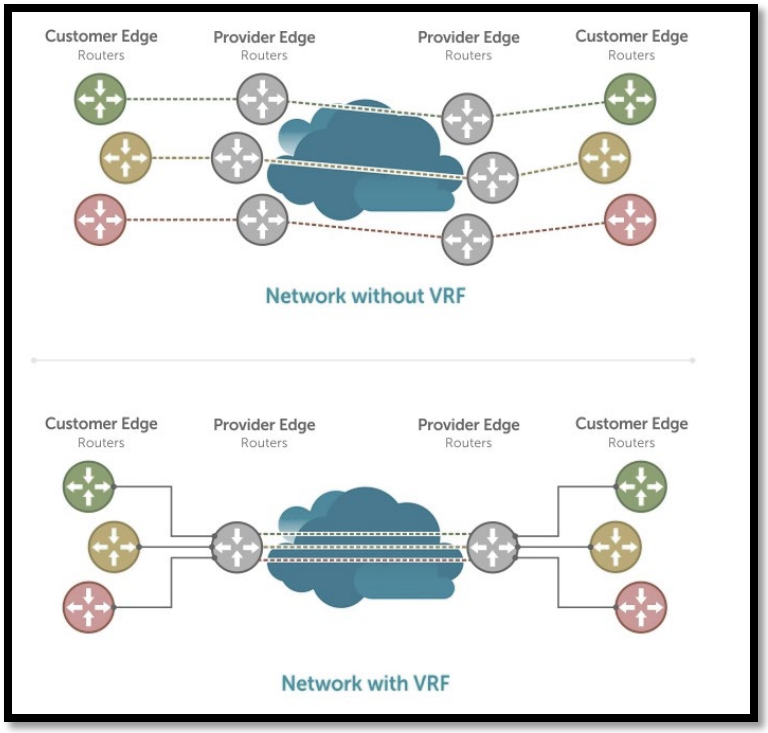
OS10 supports a management VRF instance, a default VRF instance, and a maximum of 512 non-default VRF instances. Use the default and non-default VRF instances to configure routing.

You can move the management interface from the default to management VRF instance. You need not create the management VRF instance as it already exists in the system by default.

By default, OS10 initially assigns all physical interfaces and all logical interfaces to the default VRF instance.

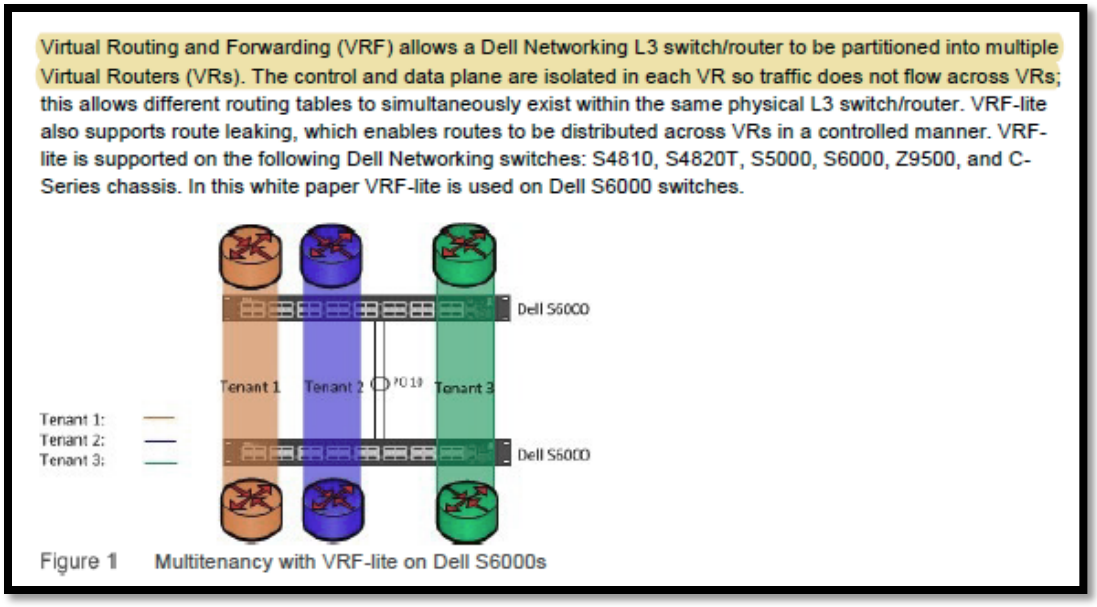
Dell EMC SmartFabric OS10 User Guide Release 10.5.0, DELL DOCUMENTATION at 471 (June 2020) (emphasis added).

123. One or more of the Dell '358 Products include a router with a second set of one or more components capable of being configured to implement a second logical router within the router. Specifically, the Dell '358 Products enable multiple logical routers to be setup within a Dell '358 Product. The below excerpt from Dell's documentation shows that interfaces for a VRF can be either physical (ethernet port or port channel) or logical (VLANs).



Dell Networking Configuration Guide for the C9000 Series Version 9.9(0.0), DELL DOCUMENTATION at 1052 (October 2015).

124. One or more of the Dell '358 Products include a router with a forwarding routing table that comprises an identifier that indicates an internal link is internal rather than an external link.



Dell Networking: Multitenancy Across Physical and Logical Environments with VRF-lite and VMware NSX – Technical White Paper, DELL DOCUMENTATION AT 4 (December 2014) (emphasis added).

125. One or more of the Dell '358 Products include a router wherein the first and second sets of components comprise functionality for establishing the internal link between the first logical router and the second logical router and advertising the internal link to other routers external to the router such that the first and second logical routers appear to the other routers as interconnected standalone routers, wherein the internal link is a logical, non-physical entity.

126. The Dell '358 Products are available to businesses and individuals throughout the United States.

127. The Dell '358 Products are provided to businesses and individuals located in the Western District of Texas.

128. Dell has directly infringed and continues to directly infringe the '358 patent by, among other things, making, using, offering for sale, and/or selling routers implementing multiple logical routers within a single physical router, including but not limited to the Dell '358 Products.

129. By making, using, testing, offering for sale, and/or selling routers implementing multiple logical routers within a single physical router, including but not limited to the Dell '358 Products, Dell has injured Plaintiffs and is liable for directly infringing one or more claims of the '358 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

130. Dell also indirectly infringes the '358 patent by actively inducing infringement under 35 USC § 271(b).

131. Dell has had knowledge of the '358 patent since at least service of this Complaint or shortly thereafter, and Dell knew of the '358 patent and knew of its infringement, including by way of this lawsuit.

132. Dell intended to induce patent infringement by third-party customers and users of the Dell '358 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Dell specifically intended and was aware that the normal and customary use of the accused products would infringe the '358 patent. Dell performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '358 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell provides the Dell '358 Products that have the capability of operating in a manner that infringe one or more of the claims of the '358 patent, including at least claim 1, and Dell further provides documentation and training materials that cause customers and end users of the Dell '358 Products to utilize the products in a manner that directly infringe one or more claims of the '358 patent.[21] By providing instruction and training to

[21] *See, e.g.*, *Dell Networking Configuration Guide for the C9000 Series Version 9.9(0.0),* DELL DOCUMENTATION (October 2015); *Dell Networking: Multitenancy with VRF-lite – Deployment and Configuration Guide*, DELL DOCUMENTATION (October 2014); *Dell Networking: Multitenancy Across Physical and Logical Environments with VRF-lite and VMware NSX – Technical White Paper*, DELL DOCUMENTATION (December 2014); *Dell EMC Networking OS10 Enterprise Edition Quick Start and Interoperability Guide - An Introduction Guide to OS10*

customers and end-users on how to use the Dell '358 Products in a manner that directly infringes one or more claims of the '358 patent, including at least claim 1, Dell specifically intended to induce infringement of the '358 patent. Dell engaged in such inducement to promote the sales of the Dell '358 Products, e.g., through Dell user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '358 patent. Accordingly, Dell has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '358 patent, knowing that such use constitutes infringement of the '358 patent.

133. The '358 patent is well-known within the industry as demonstrated by multiple citations to the '358 patent in published patents and patent applications assigned to technology companies and academic institutions. Dell is utilizing the technology claimed in the '358 patent without paying a reasonable royalty. Dell is infringing the '358 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

134. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '358 patent.

135. As a result of Dell's infringement of the '358 patent, Plaintiffs have suffered monetary damages, and seeks recovery in an amount adequate to compensate for Dell's infringement, but in no event less than a reasonable royalty for the use made of the invention by Dell together with interest and costs as fixed by the Court.

Enterprise Edition, DELL DOCUMENTATION (July 2018); *Dell EMC SmartFabric OS10 User Guide Release 10.5.0,* DELL DOCUMENTATION (June 2020); *Dell Networking S6000 10/40GbE and VMWare NSX,* DELL EMC SUPPORT YOUTUBE.COM CHANNEL (last visited June 2020), available at: https://www.youtube.com/watch?v=PIQ0fQp998c.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 8,243,593

136. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

137. Dell designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for processing a flow of a series of information packets.

138. Dell designs, makes, sells, offers to sell, imports, and/or uses Dell devices that enable the identification and penalization of data flows based on the behavior of the data flow including at least the following devices: the Dell EMC SD-WAN Edge 3000 and the Dell EMC SD-WAN Edge 600 Series (Edge 600, Edge 610, Edge 620, Edge 640, Edge 680) (collectively, the "Dell '593 Products(s)").

139. One or more Dell subsidiaries and/or affiliates use the Dell '593 Products in regular business operations.

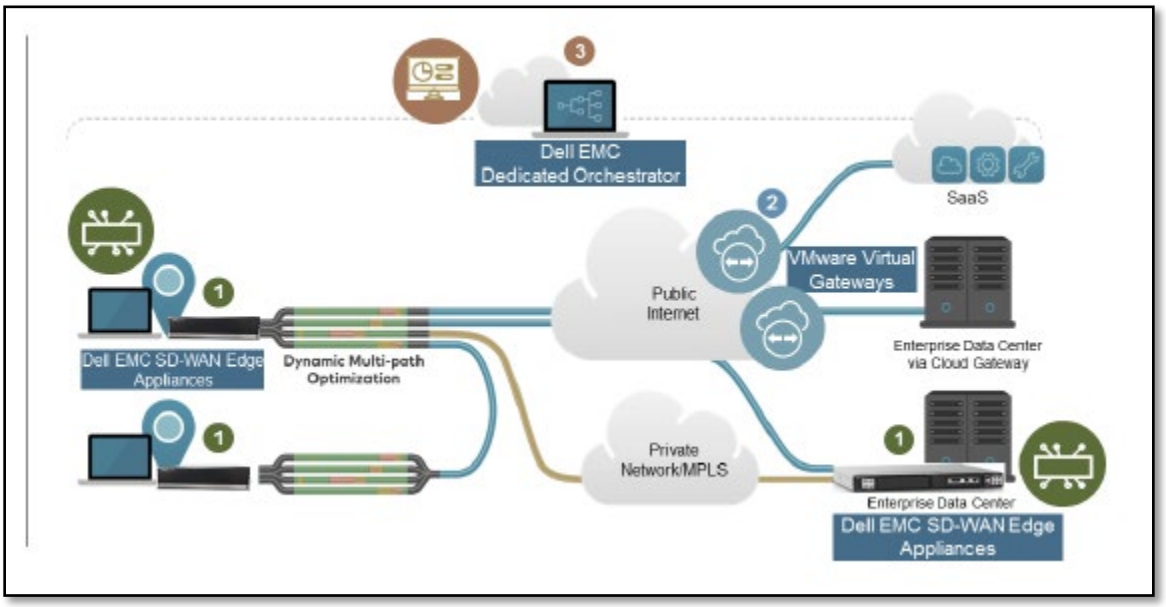
140. One or more of the Dell '593 Products include technology for processing a flow of a series of information packets. Specifically, the Dell '593 Products maintain a set of behavioral statistics based on each and every information packet belonging to a flow.

141. The Dell '593 Products are available to businesses and individuals throughout the United States.

142. The Dell '593 Products are provided to businesses and individuals located in the Western District of Texas.

143. Dell has directly infringed and continues to directly infringe the '593 patent by, among other things, making, using, offering for sale, and/or selling products and services for processing a flow of a series of information packets.

144. The Dell '593 Products maintain behavioral statistics based on the processing of packets belonging to a flow. This processing is conducted by the Dell '593 Products using "factory-integrated" VeloCloud software.



Dell EMC SD-WAN Solution Overview, DELL DOCUMENTATION at 2 (2019).

145. The Dell '593 Products maintain a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

146. The Dell '593 Products enable the generation of behavioral statistics based on each packet that is processed.

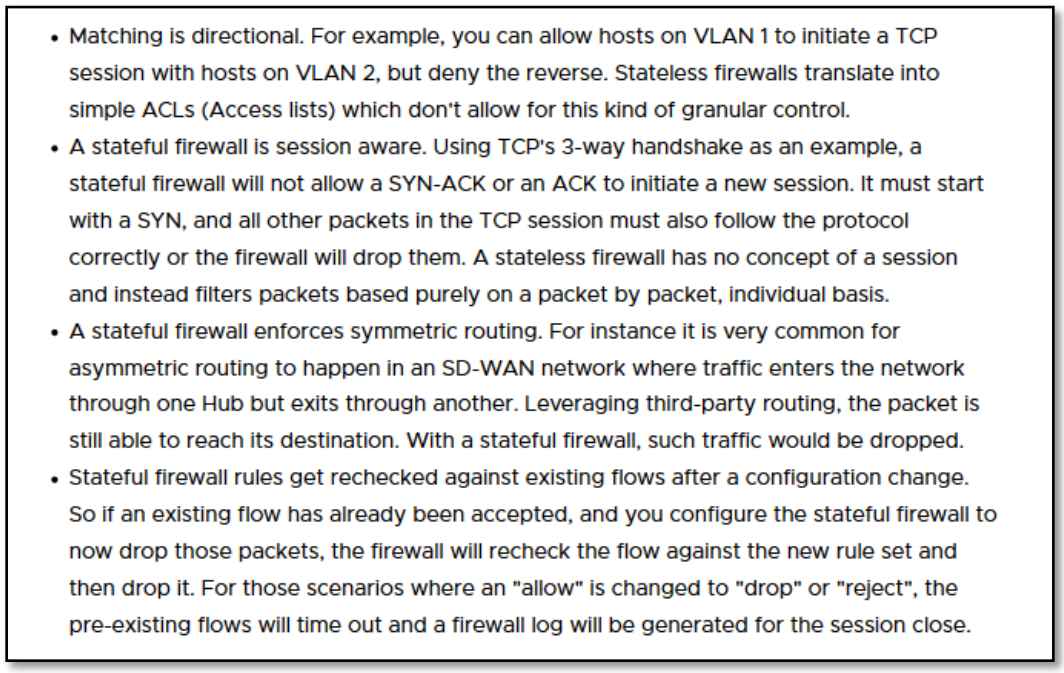
> VMware SD-WAN Edges retain the policy configuration that they get from the VMware SD-WAN Orchestrator. They determine the best link for traffic to take and act as a DHCP Server and an OSPF-BGP router. They are high-availability (HA) capable and can replace traditional routers. VMware SD-WAN Edges are enterprise-class appliances that can be provisioned with zero touch deployment. They provide secure optimized connectivity to applications in any location including private data centers, public clouds and hybrid deployments. Edges perform deep application recognition, application and packet steering, performance metrics and end to end quality of service. They can host VNF services simplifying branch office deployments of network services. Edges deliver highly available deployment with a redundancy protocol and integrate with the existing network with support for OSPF routing protocol and benefit from dynamic learning and automation. The VMware SD-WAN Edge is available as hardware-based appliances, as a virtual appliance and on the cloud marketplace on AWS and Azure. It can also be loaded in a VM on a server or as a VNF.

Guide – VMware SD-WAN by VeloCloud Features & Benefits, VMWARE DOCUMENTATION at 2 (2019) (emphasis added).

147. The Dell '593 Products determine, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

148. The Dell '593 Products determine whether the flow is exhibiting undesirable behavior regardless of the presence or absence of congestion.

149. The Dell '593 Products enable the processing of packets into flows that share "the same tuples." Documentation for the Dell '593 Products describes "[o]nce the application has been correctly identified, any future flows matching the same tuple will be reclassified automatically and hit the correct rule."



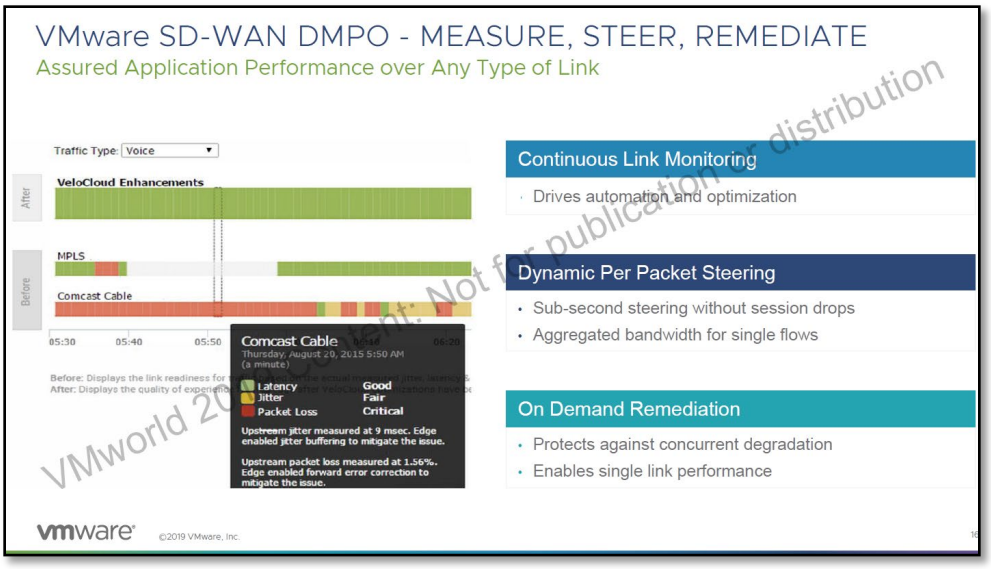
- Matching is directional. For example, you can allow hosts on VLAN 1 to initiate a TCP session with hosts on VLAN 2, but deny the reverse. Stateless firewalls translate into simple ACLs (Access lists) which don't allow for this kind of granular control.
- A stateful firewall is session aware. Using TCP's 3-way handshake as an example, a stateful firewall will not allow a SYN-ACK or an ACK to initiate a new session. It must start with a SYN, and all other packets in the TCP session must also follow the protocol correctly or the firewall will drop them. A stateless firewall has no concept of a session and instead filters packets based purely on a packet by packet, individual basis.
- A stateful firewall enforces symmetric routing. For instance it is very common for asymmetric routing to happen in an SD-WAN network where traffic enters the network through one Hub but exits through another. Leveraging third-party routing, the packet is still able to reach its destination. With a stateful firewall, such traffic would be dropped.
- Stateful firewall rules get rechecked against existing flows after a configuration change. So if an existing flow has already been accepted, and you configure the stateful firewall to now drop those packets, the firewall will recheck the flow against the new rule set and then drop it. For those scenarios where an "allow" is changed to "drop" or "reject", the pre-existing flows will time out and a firewall log will be generated for the session close.

VMware SD-WAN by VeloCloud Stateful Firewall (78116), VMWARE KNOWLEDGE BASE (March 16, 2020), available at: https://kb.vmware.com/s/article/78116.

150. Documentation for the Dell '593 Products state that as packets are processed statistics about the flow are. "Since an Edges is now session-aware, there is much more information that can be reported in the firewall logs. The logs will contain the following fields: Time, Segment, Edge, Action, Interface, Protocol, Source IP, Source Port, Destination IP, Destination Port, Rule, Bytes Received/Sent, Duration." *VMware SD-WAN by VeloCloud Stateful Firewall (78116)*, VMWARE KNOWLEDGE BASE (March 16, 2020), available at: https://kb.vmware.com/s/article/78116.

151. The Dell '593 Products enforce a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

152. The Dell '593 Products compile statistics for each flow and based on the monitoring of these statistics can take "On Demand Remediation" to penalize misbehaving flows.



Tony Banuelos and Jaspreet Bhatia, *Know, Understand, Execute: Network Monitoring and Analytics with SD-WAN,* VMWORLD 2019 SESSION NEDG2576BU PRESENTATION AT 16 (2019).

153. By making, using, testing, offering for sale, and/or selling products and services for processing a flow of a series of information packets, including but not limited to the Dell '593 Products, Dell has injured Plaintiffs and is liable for directly infringing one or more claims of the '593 patent, including at least claim 4, pursuant to 35 U.S.C. § 271(a).

154. Dell also indirectly infringes the '593 patent by actively inducing infringement under 35 USC § 271(b).

155. Dell has had knowledge of the '593 patent since at least service of this Complaint or shortly thereafter, and Dell knew of the '593 patent and knew of its infringement, including by way of this lawsuit.

156. Dell intended to induce patent infringement by third-party customers and users of the Dell '593 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Dell specifically intended and was aware that the normal and customary use of the accused products would infringe the '593 patent. Dell performed the acts that constitute induced infringement, and would induce

actual infringement, with knowledge of the '593 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell provides the Dell '593 Products that have the capability of operating in a manner that infringe one or more of the claims of the '593 patent, including at least claim 4, and Dell further provides documentation and training materials that cause customers and end users of the Dell '593 Products to utilize the products in a manner that directly infringe one or more claims of the '593 patent.[22] By providing instruction and training to customers and end-users on how to use the Dell '593 Products in a manner that directly infringes one or more claims of the '593 patent, including at least claim 4, Dell specifically intended to induce infringement of the '593 patent. Dell engaged in such inducement to promote the sales of the Dell '593 Products, e.g., through Dell user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '593 patent. Accordingly, Dell has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '593 patent, knowing that such use constitutes infringement of the '593 patent.

157. The '593 patent is well-known within the industry as demonstrated by multiple citations to the '593 patent in published patents and patent applications assigned to technology companies and academic institutions. Dell is utilizing the technology claimed in the '593 patent without paying a reasonable royalty. Dell is infringing the '593 patent in a manner best described

[22] *See e.g., Dell EMC SD-WAN Edge 600 Series Installation Guide*, DELL DOCUMENTATION (April 2020); *Dell EMC SD-WAN Edge 600 Series Setup Guide*, DELL DOCUMENTATION (August 2019); *Dell EMC SD-WAN Edge 3000 Series Setup Guide,* DELL DOCUMENTATION (August 2019); *Dell EMC SD-WAN Edge 3000 Series Installation Guide*, DELL DOCUMENTATION (August 2019); *Dell EMC SD-WAN Solution Overview*, DELL DOCUMENTATION (2019); *Dell EMC SD-WAN Solutions Overview and Demo,* TECH FIELD DAY PRESENTATION FROM DELL EMC (October 4, 2019), available at: https://www.youtube.com/watch?v=EuXsKDynAcw; and *What is SD-WAN and Why Do You Need It,* DELL YOUTTUBE.COM CHANNEL PRESENTATION (October 18, 2019), available at: https://www.youtube.com/watch?v=OF997v3H2i4.

as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

158. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '593 patent.

159. As a result of Dell's infringement of the '593 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Dell's infringement, but in no event less than a reasonable royalty for the use made of the invention by Dell together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Sable IP, LLC and Sable Networks, Inc. respectfully request that this Court enter:

A. A judgment in favor of Plaintiffs that Dell has infringed, either literally and/or under the doctrine of equivalents, the '932, '209, '358, and '593 patents;

B. An award of damages resulting from Dell's acts of infringement in accordance with 35 U.S.C. § 284;

C. A judgment and order finding that Dell's infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiffs enhanced damages.

D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiffs their reasonable attorneys' fees against Dell.

E. Any and all other relief to which Plaintiffs may show themselves to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs Sable IP, LLC and Sable Networks, Inc. request a trial by jury of any issues so triable by right.

Dated: June 26, 2020

Respectfully submitted,

/s/ Daniel P. Hipskind

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
9538 Brighton Way, Ste. 320
Beverly Hills, CA 90210
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP
114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com

Attorneys for Sable Networks, Inc. and Sable IP, LLC